I. SUMMARY OF INTERVIEW

On Tuesday, July 15, 2008, at 2:15 PM, a telephone interview was conducted between Examiner Besrour and representatives of the Applicants (Yiping Liao and Christopher Palermo). During the interview, the representatives of the Applicants discussed reasons for why Claim 1 satisfies the requirements of 35 U.S.C. § 112 and pointed out to the Examiner portions of the Specification that support Claim 1's feature of "without parsing or interpreting any data structures in the first security certificate or the second security certificate: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate". In addition, the representatives of the Applicants pointed out that this feature of Claim is not disclosed by any of the cited references. The Examiner agreed that the cited references do not disclose this feature of Claim 1 and stated that an updated search could be done based on the clarification of the claim.

II. ISSUES NOT RELATING TO PRIOR ART

Claims 1-47 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Office Action stated that "it is not clear what function can [be] performed without parsing or interpreting any data structures."

Applicants respectfully traverse.

Claim 1 recites, among other features:

> *without parsing or interpreting any data structures in the first security certificate or the second security certificate*:
>
> comparing *in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate*; and

confirming the sender's identity only when the *binary representation of the second security certificate* matches the *binary representation of the first security certificate* for the sender.

(Emphasis added.)

The Specification fully supports the features of Claim 1 listed above. Paragraph [0102] discloses that "In order to determine if two certificates are identical, however, the system does not necessarily need to know how to parse or interpret the data structure. **Instead, the system can compare the zeroes and ones of the digital certificate**". In other words, Claim 1 recites a method where a comparison of two digital certificates is performed on the binary level, without parsing or interpreting any data structures within the digital certificates themselves. The function performed by such a method is the determination of whether the two digital certificates are identical.

Paragraph [0103] and accompanying Figure 6 further detail how one embodiment of Claim 1 performs the features listed above. Figure 6 is a flow diagram that depicts a process for comparing two digital certificates. In steps 610 and 620, two certificates (i.e. certificate A and certificate B) are obtained. Then, in step 630, the lengths of the two certificates in memory are compared. If the lengths are not equal, then it is determined in step 640 that the two certificates are not identical. This determination can be made because in order for two certificates to be determined to be identical, all the bits (e.g., ones and zeroes) in one certificate must be identical to all the bits in the other certificate. Therefore, if the two certificates are of different lengths, then it would not be possible for the certificates to be identical. If the lengths are equal, however, then step 650 is performed. In step 650, all the bits in the two certificates are compared. If all the bits in one certificate are the same as all the bits in the other certificate, then it is determined in step 660 that the two certificates are identical. Else, it is determined in step 640 that the two certificates not identical. All of the steps in Figure 6 are performed without parsing or interpreting any data structure in either of the two certificates.

Finally, paragraph [0105] details the benefits of the features of Claim 1 listed above. Specifically, "[t]he benefit of the memory representation comparison is to reduce the necessity for format-specific resources. That is, since this comparison can be done independent of format, the code for implementing the system can be simpler and the expertise needed by the system implementers and administrators is reduced."

In sum, Claim 1 is fully supported and defined by the Specification, and removal of the rejection under 35 U.S.C. § 112 is respectfully requested.

III. ISSUES RELATING TO PRIOR ART

Each of the pending claims as amended recites at least one element that is not disclosed, taught, or otherwise suggested by the cited art, either individually or in combination. Accordingly, the rejections are respectfully traversed.

A. Independent Claim 1

Claim 1 stands rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *de Silva et al.* (US 6,615,347), hereinafter "*de Silva*", in view of *England et al.* (U.S. Pat. Pub. No. 2007/0174921), hereinafter "*England*". Claim 1 recites:

> *without parsing or interpreting any data structures in the first security certificate or the second security certificate*:
>
> comparing *in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate*; and
>
> confirming the sender's identity only when the *binary representation of the second security certificate* matches the *binary representation of the first security certificate* for the sender.

(Emphasis added.)

In the Office Action, the Examiner has admitted that *de Silva* does not teach or otherwise suggest the feature of "comparing in memory a binary representation of the entire second security

certificate to a binary representation of the entire firs security certificate". The Examiner also admitted during the Telephone Interview conducted on July 15, 2008, that de Silva does not teach performing a comparison of two certificates "without parsing or interpreting any data structures".

Indeed, *de Silva* is limited to using data contained **within** a digital certificate to determine whether an existing digital certificate has been changed, and thus requires advance knowledge of the digital certificate's data structure in order to access and parse the certificate serial number and/or digital signature. On the other hand, as discussed above, Claim 1 recites the comparison of binary representations of the entirety of two security certificates, without parsing or interpreting any data structures within the certificates.

The *England* reference also does not teach or otherwise suggest the features of Claim 1 emphasized above. What *England* describes is comparing a certificate **associated** with an executable binary to certificates in a list of approved certificates for verification purposes (*England* [0158]). The certificates in *England* are associated with executable binaries, but the executable binaries do not represent the certificates in any way (rather, the executable binaries represent executable software code). Moreover, *England* teaches that the comparison of certificates is performed by comparing the "certificate hashes" or other "public key representations or encodings" (see *England* paragraphs [0129], [0130], and [0132]). Therefore, *England* also does not teach "without parsing or interpreting any data structures in the first security certificate or the second security certificate, comparing in memory a binary representation of the **entire** second security certificate to a binary representation of the **entire** first security certificate" (emphasis added).

Accordingly, since neither *de Silva* nor *England*, individually or in combination, teach or otherwise suggest the limitations of comparing binary representations of the entire received digital certificate to an existing digital certificate in memory, Claim 1 is non-obvious over *de Silva* in view of *England*. Applicant respectfully requests reconsideration and withdrawal of Examiner's obviousness rejection of Claim 1.

B. Independent Claims 18, 32, 44, and 45

Independent Claims 18, 32, 44 and 45 recite features analogous to those provided in amended Claim 1. Since *de Silva* and *England* do not teach or otherwise suggest the limitations of comparing binary representations of the entire received digital certificate to an existing digital certificate in memory, Claims 18, 32, 44 and 45 are patentable over *de Silva* and *England* for the same reasons given above with respect to claim 1. Reconsideration is respectfully requested.

C. Dependent Claims 2-17, 19-31, 33-41, 43, and 47

Claims 2-17, 19-31, 33-41, 43, and 47 stand rejected under 35 U.S.C. § 103. Claims 2-17, 19-31, 33-43, and 47 depend directly or indirectly from Claims 1, 18, 32, 44, 45 and therefore include each and every feature recited in independent Claims 1, 18, 32, 44, 45. Accordingly, claims 2-17, 19-31, 33-41, 43, and 47 are allowable for the same reasons given above for claims 1, 18, 32, 44, 45. Reconsideration is respectfully requested.

D. Dependent Claim 42

Claim 42 stands rejected under 35 U.S.C. § 103(a) as allegedly obvious over *de Silva* in view of *England* in further view of US patent application publication US 2003/0037234 (hereinafter, "*Fe*").

Claim 42 depends from independent Claim 32 and therefore includes each and every feature recited in claim 32. For the reasons given above, claim 32 is patentable over *de Silva* in view of *England*. Further, *Fe et al.* fails to cure the deficiencies of *de Silva* and *England* with respect to the distinguishing features of claim 32—in particular, *Fe et al.* has no description, teaching or suggestion to perform a comparison between binary representations of security certificates. Therefore, any combination of *de Silva*, *England* and *Fe et al.* fails to provide for the complete combination that is recited in claim 42. Reconsideration is respectfully requested.

E. Dependent Claims 46

Dependent Claim 46 provides an additional comparison feature which utilizes the length in memory of the first and second digital certificates to determine whether any changes have occurred.

Claims 46 depends from independent Claim 45 and therefore includes each and every feature recited in Claim 45. Claim 45 recites the same features discussed above for claim 1 and therefore claim 45 is patentable over the cited references for the same reasons given above for claim 1. Accordingly, dependent Claim 46 is patentable over *de Silva* in view of *England* for the same reasons given above for claim 1 and also because the additional features recited in Claim are not found in *de Silva* or *England*.

The Office Action alleged that the feature of utilizing the length in memory of the first and second digital certificates for comparison is disclosed in *England*. However, while *England* discloses the comparison of certificates, it does not disclose ***how*** this comparison is performed; specifically, there is no teaching in *England* of ***utilizing lengths of certificates for comparison purposes***.

Favorable consideration is respectfully requested.

IV. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, the petition for extension of time fee and other applicable fees are submitted concurrently herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

/YipingRLiao#60301/
Yiping Liao
Reg. No. 60,301

Dated: July 16, 2008

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
(408) 414-1202
Facsimile: (408) 414-1076